RECEIVED
CENTRAL FAX CENTER
DEC 04 2007

AMENDMENTS TO THE CLAIMS

1. **(Currently Amended)** A semiconductor memory card comprising a tamper resistant module and a nonvolatile memory, wherein

the tamper resistant module includes:

an internal memory having a usage area used by a program stored in the tamper resistant module; and

a processing unit including a virtual machine and an operation system, the program being an application executed by the virtual machine, and

when requested by the program, the processing unit is operable to (i) assign an area in the nonvolatile memory to the program, and (ii) generate, on the internal memory of the tamper resistant module, access information for the assigned area, the usage area and the assigned area ~~thereby~~ composing a total area for use by the program.

2. **(Original)** A semiconductor memory card according to Claim 1, wherein

the internal memory stores a first area table indicating a location and a size of the usage area, and a second area table indicating a location and a size of the assigned area, and

the access information is the second area table.

3. **(Original)** A semiconductor memory card according to Claim 1, wherein

the processing unit comprises:

an assigning unit operable to assign, at a time of the generation of the access information, an encryption key which the program uses in accessing the assigned area;

PAGE 9/21 * RCVD AT 12/4/2007 9:29:30 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/10 * DNIS:2738300 * CSID:2027218250 * DURATION (mm-ss):03-44

an encrypting unit operable, at a time of the program writing data to the assigned area, to encrypt the data; and

a decrypting unit operable, at a time of the program reading data from the assigned area, to decrypt the data.

4. **(Original)** A semiconductor memory card according to Claim 3, wherein

the processing unit further comprises:

a receiving unit operable to receive a security level from the program; and

a storage unit that stores values for different security levels, bit lengths of an encryption key, and encryption methods, the bit lengths and encryption methods corresponding one-to-one to the values,

the encryption key assigned by the assigning unit is generated based on a bit length corresponding to the received security level, and

the encryption and decryption by the encrypting unit and decrypting unit, respectively, are performed based on an encryption method corresponding to the received security level.

5. **(Original)** A semiconductor memory card according to Claim 1, wherein

the internal memory stores a first area table indicating a location and a size of the usage area,

the nonvolatile memory stores a second area table indicating a location and a size of the assigned area, the second area table being encrypted using a predetermined encryption key, and

the access information is a set of the predetermined encryption key and information

PAGE 10/21 * RCVD AT 12/4/2007 9:29:30 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/10 * DNIS:2738300 * CSID:2027218250 * DURATION (mm-ss):03-44

indicating a location of the second area table.

6. **(Currently Amended)** A semiconductor memory card according to Claim 5, wherein

the nonvolatile memory includes a first memory module and a second memory module, and

a unit of writing in the second memory module ~~being~~ is smaller than a unit of writing in the first memory module, and the second memory module ~~storing~~ stores file management data.

7. **(Original)** A semiconductor memory card according to Claim 6, wherein

the second memory module is one of a Ferroelectric Random Access Memory and a Magnetoresistive Random Access Memory.

8. **(Currently Amended)** A semiconductor memory card according to Claim 5, wherein

the internal memory of the tamper resistant module includes a first memory module and a second memory module, and

a unit of writing in the second memory module ~~being~~ is smaller than a unit of writing in the first memory module, and the second memory module ~~storing~~ stores file management data.

9. **(Original)** A semiconductor memory card according to Claim 8, wherein

the second memory module is one of a Ferroelectric Random Access Memory and a

PAGE 11/21 * RCVD AT 12/4/2007 9:29:30 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/10 * DNIS:2738300 * CSID:2027218250 * DURATION (mm-ss):03-44

Magnetoresistive Random Access Memory.

10. **(Currently Amended)** A semiconductor memory card according to Claim 1 being a multi-application memory card, wherein

the program is one of a plurality of applications with which the memory card is compatible, and

the internal memory has a plurality of usage areas corresponding one to one to the applications.

11. **(Currently Amended)** A semiconductor memory card according to Claim 10, wherein

at a time of addition of ~~an application~~one of the applications to the memory card, the processing unit assigns an area to be used by the added application.

12. **(Original)** A semiconductor memory card according to Claim 1, wherein the assigned area is a file system in which files are stored.

13. **(Original)** A semiconductor memory card according to Claim 1, wherein the tamper resistant module includes a CPU that executes the program.

14. **(Original)** A semiconductor memory card according to Claim 1 including a host interface which is an interface with a device connected to the memory card, wherein

PAGE 12/21 * RCVD AT 12/4/2007 9:29:30 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/10 * DNIS:2738300 * CSID:2027218250 * DURATION (mm-ss):03-44

the host interface judges whether a command from the device is an expansion command, and

the program starts, if the command is judged to be the expansion command.

15. **(Currently Amended)** A semiconductor memory card of Claim 1 including ~~that comprises a tamper resistant module and a nonvolatile memory, and includes~~ a plurality of file systems, a secure level of each of the file systems being one of high, medium, and low, wherein

a first file system whose secure level is high is stored in the tamper resistant module,

a second file system whose secure level is low is stored in the nonvolatile memory, and

the total area that is a combination of the usage area and the assigned area composes a third file system whose secure level is medium ~~is stored in the nonvolatile memory, and access information for accessing the third file system is stored in the tamper resistant module~~.

16. **(Currently Amended)** A controlling program in a semiconductor memory card that comprises a tamper resistant module and a nonvolatile memory, and that is executed by a CPU in the tamper resistant module, wherein

the tamper resistant module includes: an internal memory having a usage area used by an application stored in the tamper resistant module; a virtual machine; and an operation system, the application being executable by the virtual machine, and

the controlling program is operable to (i) assign an area in the nonvolatile memory to the application, and (ii) generate, on the internal memory of the tamper resistant module, access information for the assigned area, the usage area and the assigned area ~~thereby~~ composing a total

PAGE 13/21 * RCVD AT 12/4/2007 9:29:30 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/10 * DNIS:2738300 * CSID:2027218250 * DURATION (mm-ss):03-44

area for use by the application.

PAGE 14/21 * RCVD AT 12/4/2007 9:29:30 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/10 * DNIS:2738300 * CSID:2027218250 * DURATION (mm-ss):03-44